REMARKS

I. Introduction

In response to the Office Action dated June 27, 2008, subsequent to the Amendment under 37 C.F.R. §1.111 submitted September 29, 2008, and in response to the Notice of Non-Compliant Amendment dated December 30, 2008, claims 1, 2, 8, 10, 11, 14, 15, 16, 17, 18, 24, 26, 27, 30, 31, 32, 38, 40, 41 and 44 have been amended. Claims 1-44 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for patentability or to distinguish the claims over the prior art.

III. Drawing Objections

In paragraph (5) of the Office Action, FIG. 1 was objected to because it is not clear whether the two items labeled "intermediate results 118" are necessarily the same.

Applicants' attorney has amended FIG. 1 as shown in the replacement sheet submitted herewith to overcome these objections.

IV. Specification Objections

In paragraphs (2)-(4) of the Office Action, the Abstract and the specification were objected to because of certain informalities.

Applicants' attorney has amended both the Abstract and the specification as indicated above to overcome these objections.

V. Claim Objections

In paragraph (5) of the Office Action, claims 14, 17, 30, 31 and 44 were objected to because of certain informalities.

Applicants' attorney has amended claims 14, 17, 30, 31 and 44 to overcome these objections.

In paragraph (6) of the Office Action, claim 16 was objected to as being a substantial duplicate of claim 15.

Applicants' attorney respectfully traverses this objection. Applicants' attorney notes that claim 15 is directed to a "client computer" while claim 16 is directed to a "server computer." Because the server computer performs different recited functions than the client computer, claim 16 is not a duplicate of claim 15. Consequently, Applicants' attorney requests that the objection be withdrawn.

VI. Statutory Subject Matter Rejections

In paragraphs (7)-(8) of the Office Action, claims 17-44 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Applicants' attorney has amended claims 17 and 31 to overcome these rejections.

However, should issues still remain in this regard, Applicants' attorney requests that the Examiner indicate how the rejection can be overcome, in accordance with the directives of the Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility (Interim Guidelines) II, and as set forth in M.P.E.P. §2106. Specifically, should it be necessary, the Applicants' attorney requests that the Examiner identify features of the invention that would render the claimed subject matter statutory if recited in the claim. See Interim Guidelines IV.B, and M.P.E.P. §2106.

VII. Rejections under 35 U.S.C. §112, First Paragraph

In paragraphs (9)-(10) of the Office Action, claims 1-44 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. Specifically, the Office Action asserts the following:

> A determination of a failure to comply with the enablement requirement is made considering the undue experimentation factors set forth in MPEP § 2164.01 (a). In the present application, the factors that appear to weigh most heavily are the breadth of the claims (MPEP § 2164.08), the amount of direction provided by the inventor (MPEP § 21 64.03), and the existence of working example (MPEP § 2164.02). Independent Claims 1, 15, 16, 17, and 31 each broadly recite the limitation "in order to produce actual results" or "producing actual results". Dependent Claims 9, 25, and 39 also recite the limitation "in order to produce actual results". These limitations constitute an extremely broad recitation of a

description of results produced. However, there is nothing in the specification that suggests what might distinguish "actual" results from any other results that are produced. The only descriptions in the specification largely use the same language as is present in the claims. These descriptions clearly do not provide a working example, other than to suggest that the actual results are displayed to the user (page 8, line 9 of the specification). This indicates that there is little direction provided by the inventor and no clear working example. Combined with the broad recitations of the claims, this suggests that the enablement of the description is not commensurate in scope with the claims (MPEP § 2164.08) and that undue experimentation would be required to make or use the invention based on the disclosure (MPEP § 2164.06).

Applicants' attorney respectfully traverses this objection. Applicants' specification provides fully enabling description of the phrase "actual results." Consider, for example, the description in Applicants' specification set forth at page 7, line 12, as amended, which is reproduced below:

> FIG. 1 is block diagram that illustrates the basic architecture and control flow of the preferred embodiment of the present invention. This architecture is known as the "database as a service" (DAS) model, which involves trusted clients and an untrusted server.
>
> In this illustration, there are three fundamental entities. A client computer 100 encrypts data and stores the encrypted data at a server computer 102 in an encrypted client database 104 managed by an application service provider 106. The encrypted client database 104 is augmented with additional information (which we call the index) that allows certain amount of query processing to occur at the server computer 102 without jeopardizing data privacy. The client computer 100 also maintains metadata 108 which is used by a query translator 110 for translating the user query 112 into different portions, i.e., a query over encrypted data 114, for execution on the server computer 102, and a query over decrypted data 116, for execution on the client computer 100. The server computer 102 generates an encrypted intermediate results set 118a, which is transferred to the client computer 100 and stored as temporary results 120. The client computer 100 includes a query executor 122 that decrypts the temporary results 120 and performs the query over decrypted data 116, which may include a filtering or sorting operation, to generate an updated intermediate results set 118b, which is then re-encrypted and transferred back to the server computer 102. The server computer 102 completes its query processing on the re-encrypted intermediate results set 118b, in order to generate a new intermediate results set 118c, which is provided to the client computer 100 and stored as temporary results 120. Finally, the query executor 122 in the client computer 100 decrypts the temporary results 120 and performs the query over decrypted data 116 in order to generate actual results 124 for display 126 to the user. (Emphasis added.)

Applicants' attorney notes that there are five types of "results" described and labeled with reference numbers in the Applicants' specification, including "encrypted intermediate results set 118a," "updated intermediate results set 118b," "re-encrypted intermediate results set 118c," "temporary results 120," and "actual results 124." Moreover, in the context of the above portion of Applicants' specification, "actual results 124" comprise are generated by the final query performed by a client computer over the decrypted temporary results 120. These temporary results 120 are, initially, encrypted intermediate results set 118a generated by the server computer 102, which are transferred to the client computer 100 and stored as temporary results 120. The client computer 100 decrypts the temporary results 120 and performs a query over decrypted data 116, which may include a filtering or sorting operation, to generate an updated intermediate results set 118b. The updated intermediate results set 118b is then re-encrypted and transferred back to the server computer 102. The server computer 102 completes its query processing on the re-encrypted intermediate results set 118b, in order to generate a new intermediate results set 118c. The new intermediate results set 118c is provided to the client computer 100 and stored, again, as the temporary results 120. Finally, the client computer 100 decrypts the temporary results 120 and performs a query over the decrypted temporary results 120 in order to generate "actual results 124" for display 126 to the user.

In view of the above, Applicants' attorney respectfully submits that Applicants' specification provides a fully enabling description of the phase "actual results." Consequently, Applicants' attorney requests that the objection be withdrawn.

VIII. Rejections under 35 U.S.C. §112, Second Paragraph

In paragraphs (11)-(12) of the Office Action, claims 1-44 were rejected under 35 U.S.C. §112, second paragraph, for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, on various grounds.

With regard to claims 1, 15, 16 and 17, and the use of the pronoun "it," Applicants' attorney has amended the claims to overcome these rejections.

With regard to claims 1, 9, 15, 16, 17, 25, 31, and 39, and the recitation of the limitation "to produce actual results" or "producing actual results," which the Office Action asserts is generally unclear, as it is not clear how "actual results" are distinguished from any other results, such as the intermediate results set, or any other results of any of the functions performed by the

claimed system, and further, where the Office Action asserts that there is nothing in the claims or specification that defines or distinguishes "actual results" from any other results, which renders the claim indefinite, Applicants' attorney respectfully traverses these rejections. In this regard, Applicants' attorney cites to the arguments set forth in section VII above.

With regard to claims 2, 18 and 32, which recite several additional functions (decrypting, performing operations, re-encrypting, and returning) that the system performs, the Office Action asserts that it is not clear at what point (i.e. in what order) these operations are to be performed, which renders the claim indefinite. Applicants' attorney respectfully traverses these rejections. Applicants' attorney notes that the language of the claims clearly specifies an order for the operations, namely decrypting the set, performing operations on the decrypted set to generated an updated set, re-encrypting the updated set, and sending the re-encrypted set to the server.

With regard to claims 6, 9, 17, 18, 22, 25, 31, 32, 36 and 39, which recite the limitation "intermediate results set," the Office Action states that it is not clear to which of the intermediate results sets the limitation is intended to refer. Applicants' attorney has amended the claims to overcome these rejections.

With regard to claims 8, 10, 24, 26, 38, 40, which recite the limitation "different placements of the ... operator" within execution plans, the Office Action asserts that it is not clear exactly what is intended by the use of the term "placements," and that it is not clear if this is intended to refer to an ordering, either temporal or spatial or otherwise, of the operator, or to another sort of placement. Applicants' attorney respectfully traverses these rejections. Applicants' specification describes the different placements of the referenced operators in a query tree, as set forth below:

> Applicants' specification: page 21, line 14 et seq.
> **It is obvious that a rich set of possibilities exist for placing Δ and ω operators in a query tree, and that different placements of those operators can result in different query execution plans, which may have significantly different resource utilization and consumption.** Therefore, the decision on a query execution plan should be made judiciously based on some criteria that considers system and application specific requirements.

Indeed, Applicants' attorney notes that the Applicants' specification goes into great detail concerning the optimal placement of a "round-trip filtering operator" and a "last-trip decryption operator" in a query tree.

With regard to claims 8, 10, 11, 24, 26, 27, 38, 40 and 42, which recite the limitation "optimizes placement," the Office Action asserts that there is no standard set forth with respect to which the optimization is performed, and this is a relative term for which no basis or standard of comparison has been clearly set forth in the claims or specification. Applicants' attorney has amended the claims to overcome these rejections, but nonetheless respectfully traverses these rejections. Applicants' attorney notes that the Applicants' specification, at page 21, line 14, set forth above, states that different placements may have significantly different resource utilization and consumption.

In paragraph (13) of the Office Action, claims 17-44 were rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps, wherein the omitted steps are "decrypting the intermediate results set." Applicants' attorney has amended the claims to overcome these rejections.

IX. Requirement for Information under 37 C.F.R. §1.105

On pages 20-21 of the Office Action, applicants and the assignee of this application were required under 37 C.F.R. §1.105 to provide the following information that the Examiner has determined is reasonably necessary to the examination of this application.

In response to this requirement, the Office Action asked that answers be provided to each of the following interrogatories eliciting factual information:

> In general, where in the parent application (Serial No. 10/449,421) is support found for the claim limitations, particularly those of the independent claims? More specifically, where is support (i.e. enabling written description as per 35 U.S.C. 112, first paragraph) in the parent application found for the limitations in independent Claim 1 regarding returning intermediate results to the server computer and sending the intermediate results back again to the client computer, and the more detailed related limitations of dependent Claim 2? Similarly, where is support in the parent application found for the corresponding limitations of independent Claims 15 and 16? Where is support in the parent application found for corresponding limitations in independent Claims 17 and 31 regarding re-encrypting updated intermediate results and transferring the re-encrypted intermediate results to the server and transferring the new intermediate results back to the client, and the more detailed related limitations of dependent Claims 18 and 32?

Applicants' attorney respectfully submits that support for the claim limitations can be found in the specification of the parent application at least at the following locations:

Parent Application specification: page 5, line 18 et seq.

1. Overview

FIG. 1 is block diagram that illustrates the basic architecture and control flow of the preferred embodiment of the present invention. This architecture is known as the "database as a service" (DAS) model, which involves trusted clients and an untrusted server.

In this illustration, there are three fundamental entities. A client computer 100 encrypts data and stores the encrypted data at a server computer 102 in an encrypted client database 104 managed by an application service provider 106. The encrypted client database 104 is augmented with additional information (which we call the index) allows certain amount of query processing to occur at the server computer 102 without jeopardizing data privacy. The client computer 100 also maintains metadata 108 which is used by a query translator 110 for translating the user query 112 into different portions, i.e., a query over encrypted data 114, for execution on the server computer 102, and a query over decrypted data 116, for execution on the client computer 100. The server computer 102 generates an encrypted intermediate results set 118, which is provided to the client computer 100 and stored as temporary results 120. The client computer 100 includes a query executor 122 that decrypts the temporary results 120 and performs the query over decrypted data 116 in order to generate actual results 124 for display 126 to the user.

Specifically, data from a client computer 100 is encrypted by the client computer and hosted by a server computer 102, the encrypted data is operated upon by the server computer 102, using one or more operators selected from a group of operators comprising: (a) inequality logic operators, (b) aggregation operators, and (c) wildcard matching operators, to produce an encrypted intermediate results set 118, the encrypted intermediate results set 118 is sent from the server computer 102 to the client computer 100, and the intermediate results set 118 is decrypted and filtered by the client computer 100 to produce actual results. In this logic, the group of operators is limited because the encrypted intermediate results set 118, when decrypted, includes inaccuracies therein. Moreover, the client computer 100 applies a set of correction procedures to the decrypted intermediate results set 118 to remove the inaccuracies therein.

In this environment the client computer 100 maintains the needed encryption key(s), and the data is encrypted by the client computer 100 before it is sent to the server computer 102 for inclusion in the encrypted client database 104. Consequently, the data is always encrypted when it is stored on or processed by the server computer 102. Moreover, at no time are the encryption keys given to the server computer 102, and thus the data can never be decrypted by the server computer 102.

Parent Application specification: page 23, line 1 et seq.

5. Query Splitting

Given a query Q, our purpose in this section is to develop a strategy to split the computation of Q across the server and the client. The server will use the implementation of the relational operators discussed in the previous section to compute as much of the query as possible, relegating the remainder of the computation to the client. Our objective is to come up with the "best" query plan for Q that minimizes the execution cost. In our setting, the cost of a query consists of many components – the I/O and CPU cost of evaluating the query at the server, the network transmission cost, and the I/O and CPU cost at the client. A variety of possibilities exist. For example, consider the following query over the *emp* table that retrieves employees whose salary is greater than the average salary of employees in the department identified by *did*=1.

```
SELECT emp.name FROM emp
WHERE  emp.salary > (SELECT AVG(salary)
FROM emp WHERE did = 1);
```

The corresponding query tree and some of the evaluation strategies are illustrated in FIGS. 4(a) to (d). The first strategy (FIG. 4(b)) is to simply transmit the *emp* table to the client, which evaluates the query. An alternative strategy (FIG. 4(c)) is to compute part of the inner query at the server, which selects (as many as possible) tuples corresponding to (*did*=1). The server sends to the client the encrypted version of the *emp* table, i.e., emp^S, along with the encrypted representation of the set of tuples that satisfy the inner query. The client decrypts the tuples to evaluate the remainder of the query. **Yet another possibility (FIG. 4(d)) is to evaluate the inner query at the server. That is, select the tuples corresponding to the employees that work in department *did*=1. The results are shipped to the client, which decrypts the tuples and computes average salary. The average salary is encrypted by the client and shipped back to the server, which then computes the join at the server. Finally, the results are decrypted at the client.**

Applicants' attorney respectfully submits that the above portions of parent application provide an enabling written description, as per 35 U.S.C. §112, first paragraph, for the limitations in claims 1, 2, 15, 16, 17, 18, 31 and 32.

Further in response to this requirement, the Office Action asked that copies of each publication which any of the Applicants authored or co-authored and which describe the disclosed subject matter of the present application be provided.

Applicants' attorney submits herewith a publication entitled "Query Optimization in Encrypted Database Systems," by Hakan Hacigumus, Bala Iyer and Sharad Mehrotra (the Applicants of the present application), which was published in Proceeding of 10th Database

Systems for Advanced Applications Conference, April 2005, pp. 43-55. Applicants' attorney notes that this publication is dated after the filing date of the present application. Applicants' attorney is presenting two copies of the publication: a photocopy of the publication as published and a "clean" copy of the same publication in a more readable form.

X. Prior Art Rejections

In paragraphs (15)-(16) of the Office Action, claims 1-44 were rejected under 35 U.S.C. §102 as being anticipated by Hacigumus et al., "Executing SQL Over Encrypted Data in the Database-Service-Provider Model" (Hacigumus).

Applicants' attorney respectfully traverses the rejections.

As noted above, portions of the parent application provide an enabling written description, under 35 U.S.C. §112, first paragraph, for the limitations in at least independent claims 1, 15, 16, 17 and 31. Thus, at least these claims are entitled to a priority date at least as early as the filing date of the parent application, namely May 30, 2003.

Applicants' attorney submits herewith copies of the Declarations under 37 C.F.R. §1.132 previously submitted in the parent application stating that the Hacigumus comprises a description of the Applicants' invention, and that the publication was made on behalf of the Applicants. It is noted that the Hacigumus reference was published on June 4-6, 2002, which is less than one year prior to the May 30, 2003 filing date of the parent application.

Consequently, the Hacigumus reference is not a prior art reference under 35 U.S.C. §102(a) against at least independent claims 1, 15, 16, 17 and 31. Thus, Applicants' attorney requests that the rejections of the claims on these grounds be withdrawn.

XI. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

It is believed that no fees are due at this time. Nonetheless, should any charges be deemed necessary, please charge any such fees, or credit any overpayments, to Deposit Account No. 09-0460 of IBM Corporation, the assignee of the present application.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: January 30, 2009

By: /George H. Gates/
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30571.295-US-I1